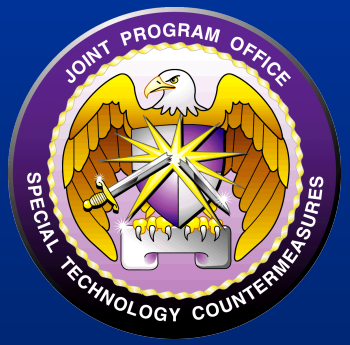


Joint Program Office for Special Technology Countermeasures

J
P
O

S
T
C

Control Systems Vulnerabilitie

Tri-Service Power Expo 2003

National Defense Industrial Association
15-17 July 2003
Norfolk, Virginia

Briefing Classification:

UNCLASSIFIED

Contact Information

Joint Program Office for Special Technology Countermeasures

Naval Surface Warfare Center, Dahlgren Division

Dahlgren, VA 22448-5100

Mike Burks

(540) 653-4973

burksmw@nswc.navy.mil

UNCLASSIFIED

UNCLASSIFIED

Agenda

- Types of Control Systems
- Architecture
- Impact of Disruption
- Reducing Vulnerabilities

UNCLASSIFIED

Supervisory Control and Data Acquisition

SCADA

- Used in Electric Power, NG, POL, Water, Waste Water
- Older Systems - Primary Conduits of Raw Data In and Commands Out
- Newer Systems - Process and Store Significant Amount of Data Internally
- Local Control Augmented by Centralized Control Using SCADA

UNCLASSIFIED

Distributed Control Systems

DCS

- Control Large Manufacturing and Production Facilities
- Process and Store Significant Amount of Data
- Chemical Plant Processes Monitoring
- Power Plant DCS Linked to Energy Management Center
- Power Plant DCS Vulnerabilities Can Extent to Control Center

UNCLASSIFIED

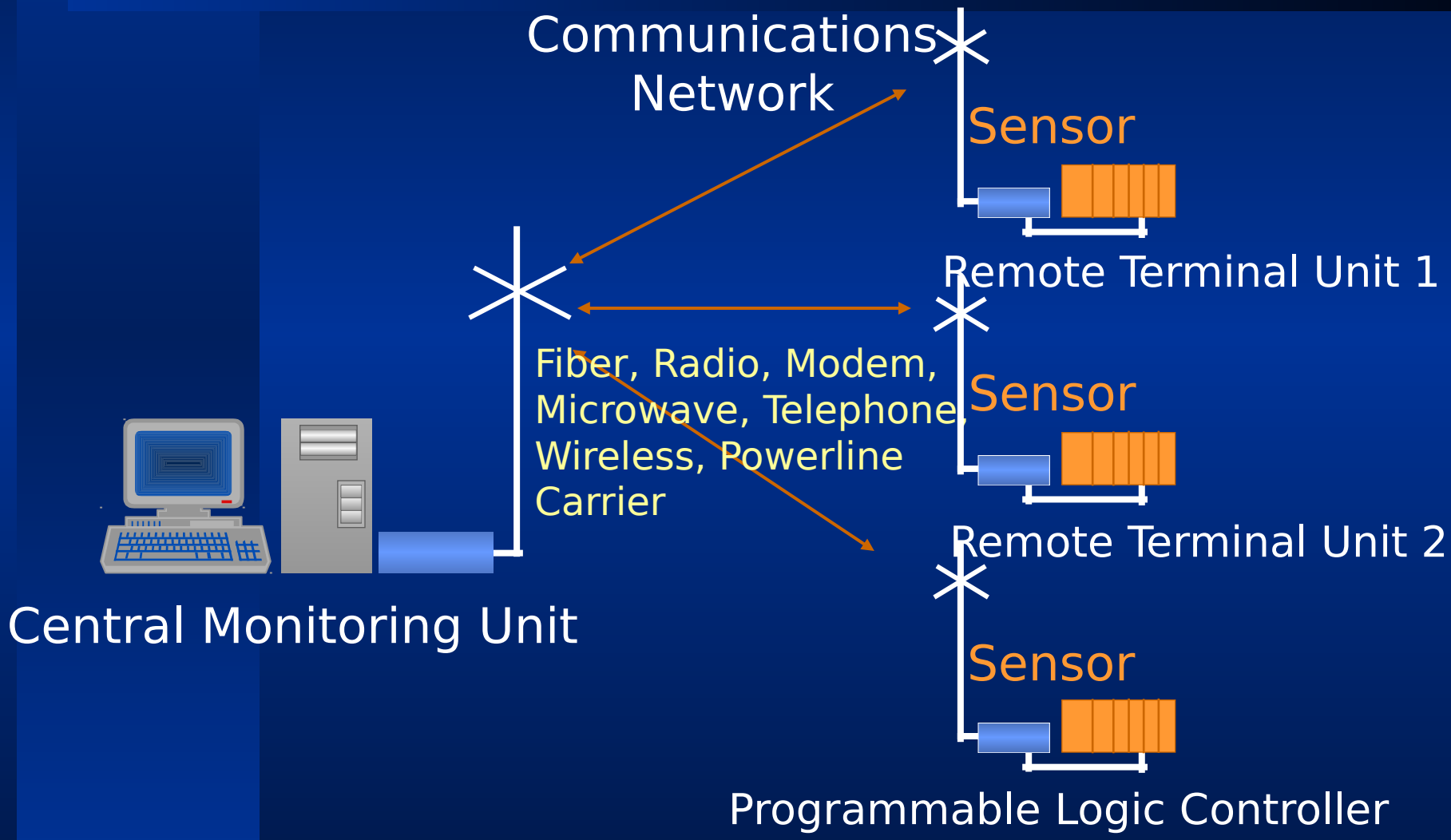
Programmable Logic Controllers

PLC

- Used in Manufacturing Facilities, Industrial Facilities, Power Plants,Substations, Water Facilities, US NAVY Warships
- May Be used as a Remote Terminal Unit (RTU) for SCADA
- Older Systems - PLC Impact Localized
- Newer Systems - PLC Impact Widespread
- Networking PLC will Increase Vulnerabilities

UNCLASSIFIED

Control System Architecture



UNCLASSIFIED

Requirements

- Highly Reliable
- Make Automated Changes to Processes
- Use Real Time Operating System
- High Performance
- High Functionality

UNCLASSIFIED

Polled Communications System

Polled System

- Master Polls Slaves in Sequence
- Slave Responds Only If Requested (Half-Duplex)
- No Digital Collisions on Network
- Slave To Master To Slave Communications

UNCLASSIFIED

Interrupt Communications Systems

Interrupt System (Report By Exception)

- Slave Monitors Inputs and Initiates Report Based On Change
- Erratic System Operation Caused by Digital Collisions on Network
- Master Polls After Slave Fails to Transmit
- Slave To Slave Communication

UNCLASSIFIED

Software Vulnerabilities

- Use Insecure Industry-Wide Protocols (DNP3.0, Modbus, Profibus, etc.)
- Relying On Obscurity for Security
- Heavy Use of Clear Text or ASCII
- Protocol Analyzers Available to Decode Structures
- Architectures Common Across All Industries
- Operating Systems DOS, VMS, UNIX, NT, LINUX, SOLARIS
- Proprietary Software Discussed at Conferences and Periodicals
- Security Patches Impact Functionality and Performance

UNCLASSIFIED

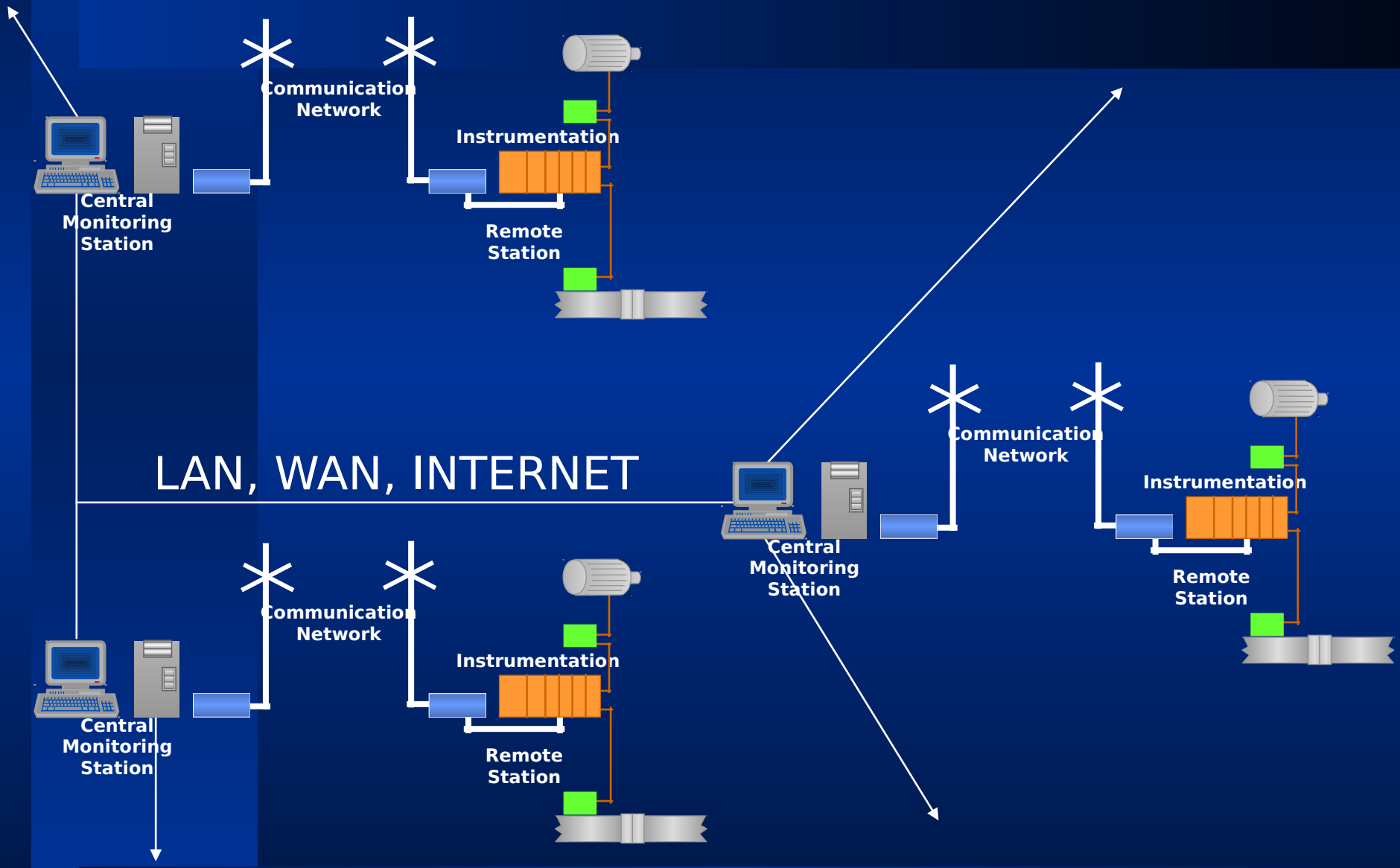
Representative RF Threats

Surplus Military RF Devices

Man Portable RF Devices

UNCLASSIFIED

Corporate Architecture



UNCLASSIFIED

Corporate Network

- Highly Networked System
- Easy Access to Control Systems From Corporate Intranet
- Few Firewalls and Intrusion Detection at Operational Facilities
- (Power Plants & Substations)
- Remote Maintenance Performed by Vendors
- Direct Remote Access Not Protected by Corporate Security

UNCLASSIFIED

Impacts of Disruptions

Depends on Level of Sophistication of Intrusion

Electric Power

- Outages (Hours to Days) and Equipment Damage
- Revert to Manual Operation of System
- Monetary

Chemical/LNG

- Safety Related Safeguards Interrupted
- Potentially Catastrophic
- Monetary

UNCLASSIFIED

Impacts of Disruptions

Depends on Level of Sophistication of Intrusion

Telecommunications

- Loss of Service (Hours) and Equipment Damage
- Monetary

Water and Wastewater

- Contamination
- Public Confidence
- Monetary

Manufacturing

- Equipment Damage
- Monetary

UNCLASSIFIED

Example of Impact

Bellingham, Washington June 1999

- Pressure surge occurred during SCADA slowdown
- Control Room Operator Unable to Relieve Pressure
- 237,000 gallons of gasoline released from ruptured 16 “ gasoline pipeline
- SCADA data base modifications made before event
- System Administrator saw errors 18 minutes before rupture
- System Administrator did not notify operators
- Remote dialup access to SCADA for account holders
- Findings by National Transportation Safety Board faulted database modification

UNCLASSIFIED

Reducing Vulnerabilities (Short Term)

- Assume All Control Systems are Vulnerable to Attack
- Eliminate Back Doors Used For Maintenance
- Implement a Business to Control System Security Policy
- Limit Access to Control Systems
- Install Security Patches and Insist Vendors Do the Same
- Install Firewalls and Intrusion Detection

UNCLASSIFIED

Reducing Vulnerabilities (Long Term)

Information Sharing Between Industries, (ISACs), and Government

Support Development of Control System Security Technology

- Specifying Security Technology in New Purchases
- Firewalls
- Intrusion Detection
- Encryption
- Secure Real Time Operating Systems

Join Technical Organizations and Consortiums to Influence Industry

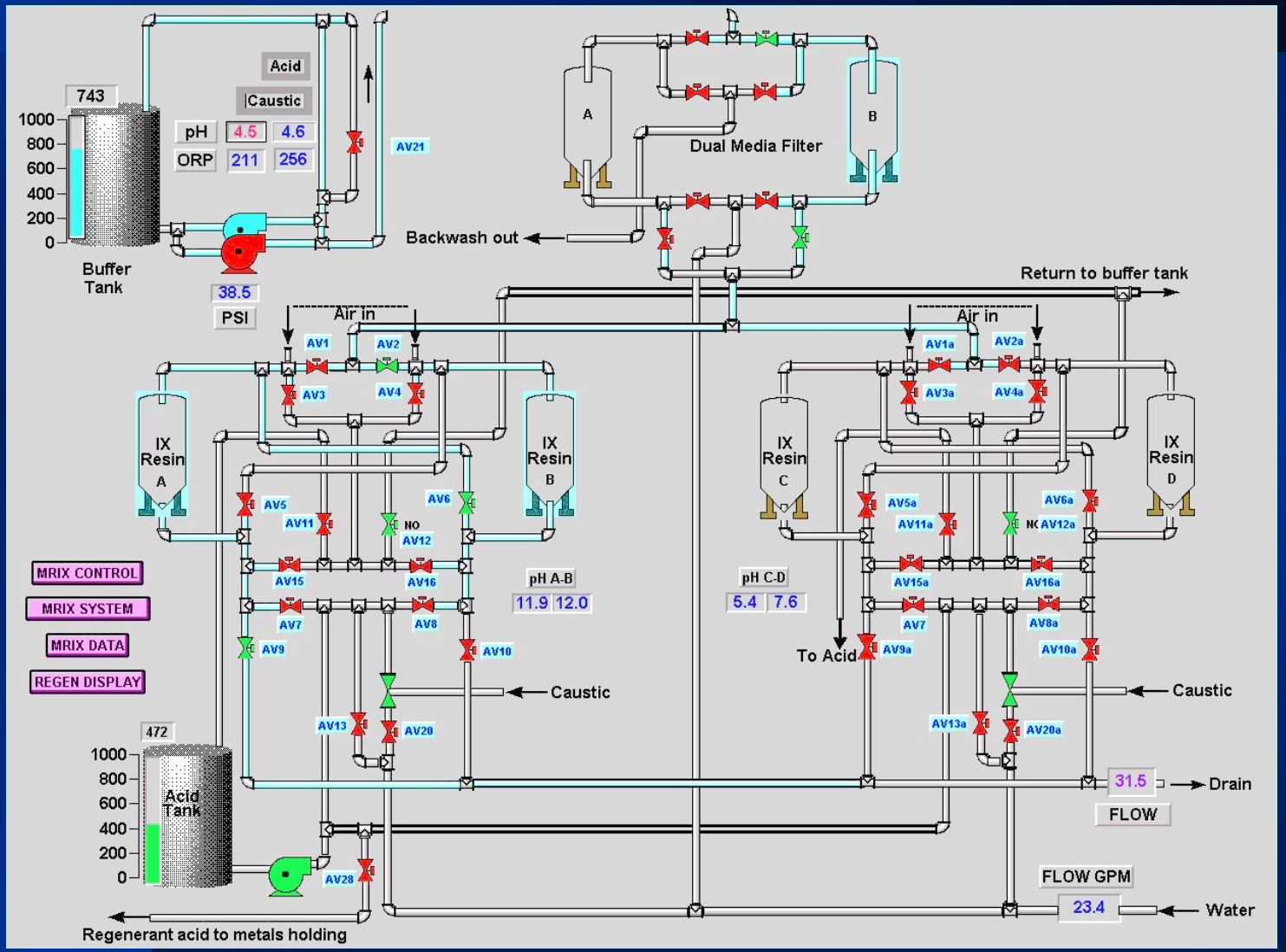
- Consortium for Electric Infrastructure to Support a Digital Society (CEIDS)
- IEEE-Instrument, Systems and Automation Society (IAS)
- International Electrotechnical Commission (IEC)

UNCLASSIFIED

Dahlgren Test Bed

UNCLASSIFIED

Questions ?



UNCLASSIFIED